

Fig. 1

00420430-100199

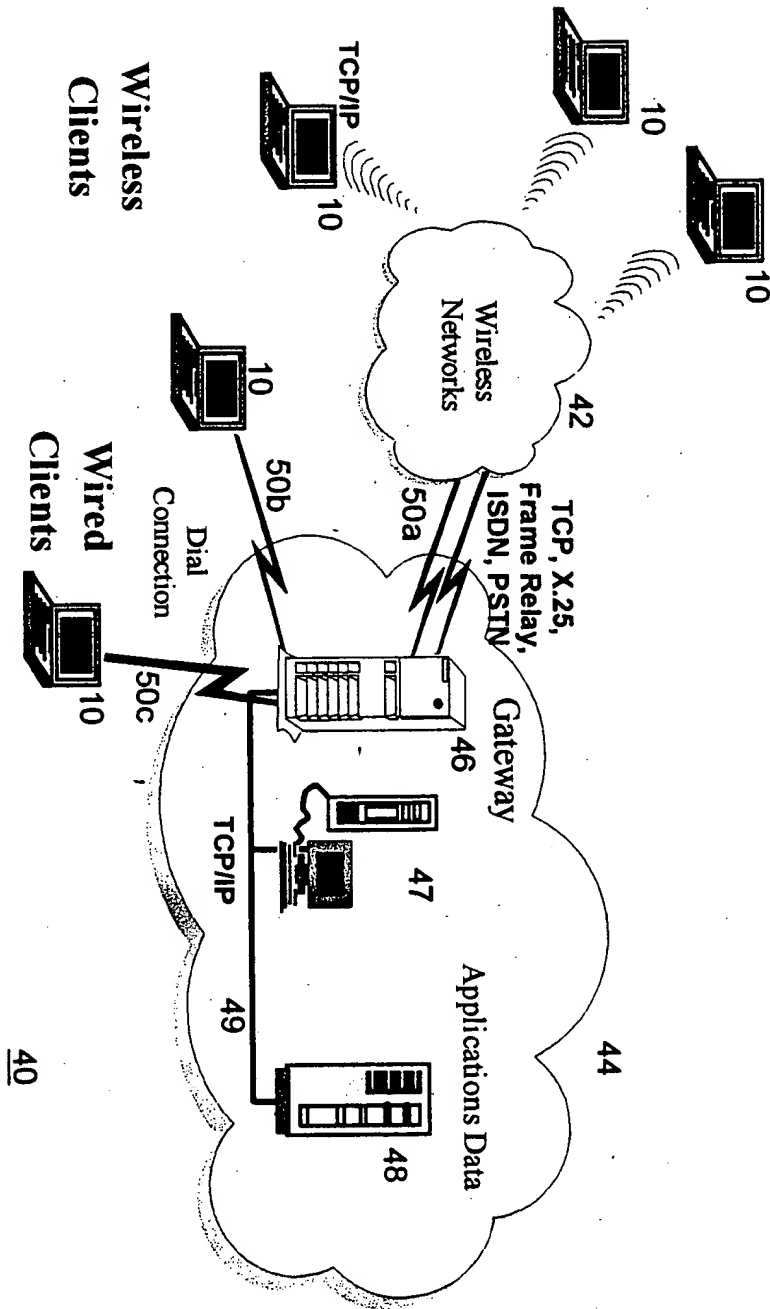


Fig. 2
(Prior Art)

09422430-102409

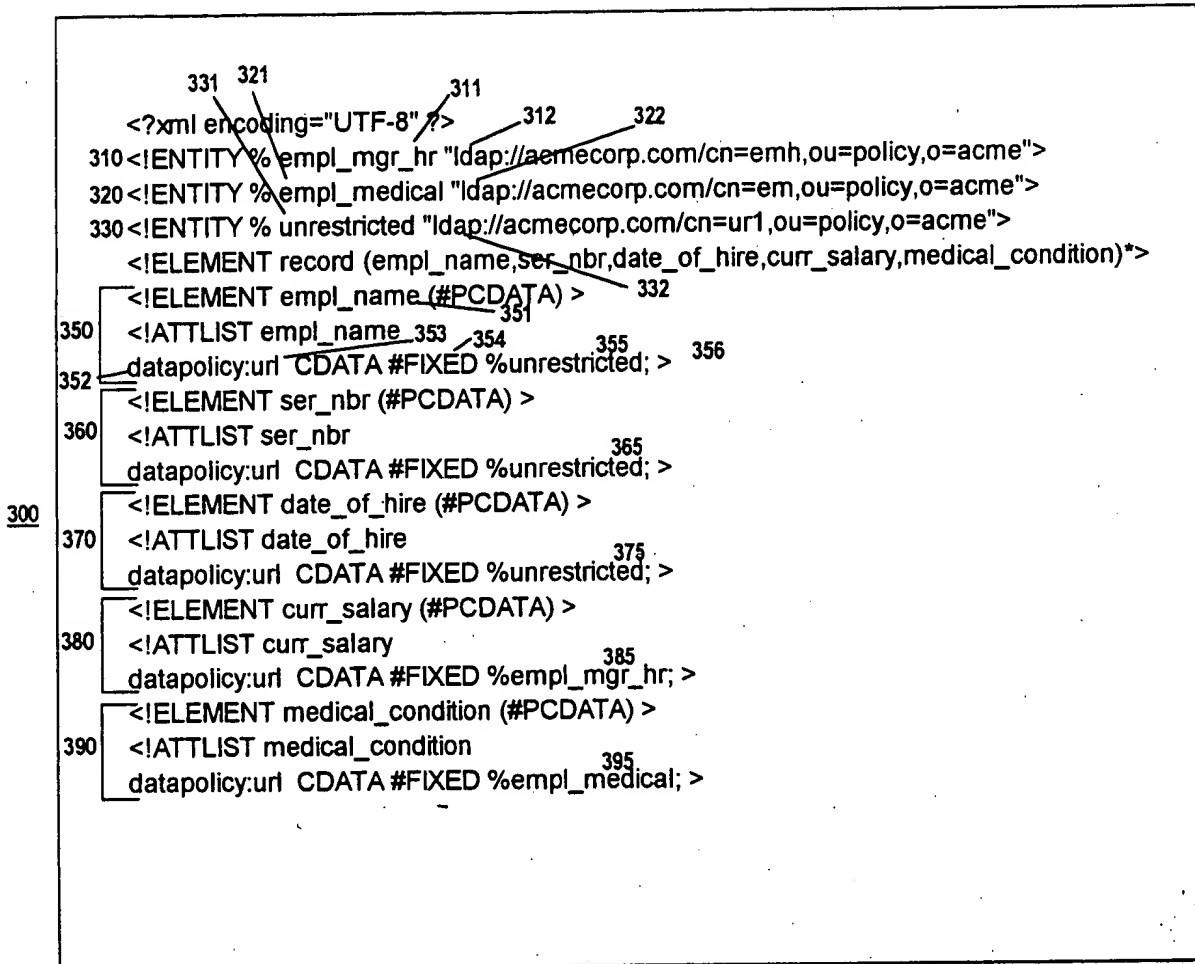


Fig. 3



400

```
<? xml version="1.0" encoding ="UTF-8" ?>
<!DOCTYPE record SYSTEM "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >
<empl_name>
John Q. Smith
</empl_name>
<ser_nbr>
E135246
</ser_nbr>
<date_of_hire>
01/01/1980
</date_of_hire>
<curr_salary>
3395.00
</curr_salary>
<medical_condition>
diabetic
</medical_condition>
```

405

402

404

406

408

410

Fig. 4A

661201-0122160

420

431 <? xml version="1.0" encoding="UTF-8" ?>
430 <!DOCTYPE record SYSTEM "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >
432 <encrypt: class name="1" type="3DES" len="168" tempkey="MjdqcmhlQHvzLmlibS5jb20xRzB">
433 <encrypt: key DN="cn=managers,ou=groups,o=acme" KeyIdentifier="MIIGEjCCBbygAwIBAgIKFZrHywAQ"
Ekey="QAAAAAAZANBgkqhkiG9w0BAQUFAD"/>
432 <encrypt: key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSib3DQJEJARYbYm9zc0BicnFQ"
Ekey="QudGlucmFsZWlnaC5pYm0uY29tMQ"/>
433 <encrypt: key DN="cn=hr,ou=groups,o=acme" KeyIdentifier="DlbQzc0BEYbCicnFSqGS3YJmAR9Q"
Ekey="sGQFIYcmWtMlnaC2u5ZudpYm9Q0u"/>
</encrypt: class>
441 <encrypt: class name="2" type="BLOWFISH" len="128" tempkey="AHIACQBuaHQAYgAuAHIAYQ">
440 <encrypt: key DN="cn=doctors,ou=groups,o=acme" KeyIdentifier="QTA5MDMyMDQOMTZaFw0wMDA5MDI"
Ekey="EgYDVQQLLEwdSYWxlaWdoMR"/>
442 <encrypt: key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSib3DQJEJARYbYm9zc0BicnFQ"
Ekey="EwJVUzELMAkGA1UECBMCTk"/>
</encrypt: class>

<empl_name>
John Q. Smith
</empl_name>
<ser_nbr">
E135246
</ser_nbr>
<date_of_hire>
01/01/1980
</date_of_hire>
<curr_salary>
422 <encrypt: data class="1">
3395.00 423
</encrypt: data>
</curr_salary>
<medical_condition>
424 <encrypt: data class="2">
diabetic 425
</encrypt: data>
</medical_condition>

Fig. 4B

450

450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473

```

<? xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE record SYSTEM "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >

<encrypt:class name="1" type="3DES" len="168">
  <encrypt:key DN="cn=managers,ou=groups,o=acme" KeyIdentifier="MlIGEjCCBbygAwIBAgIKFZrHywAQ"
    Ekey="QAAAAAAZANBgkqhkiG9w0BAQUFAD"/> 475
  <encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSib3DQEJARYbYm9zc0BicnFQ"
    Ekey="QudGlucmFsZWlnaC5pYm0uY29tMQ"/> 476
  <encrypt:key DN="cn=hr,ou=groups,o=acme" KeyIdentifier="DlbQzc0BEYbCicnFSqGS3YJmAR9Q"
    Ekey="dpYmGmFsZWlnaC5pYm0uY29tMQ"/> 477
</encrypt:class>

<encrypt:class name="2" type="BLOWFISH" len="128">
  <encrypt:key DN="cn=doctors,ou=groups,o=acme" KeyIdentifier="QTA5MDMyMDQ0MTZaFw0wMDA5MDI"
    Ekey="EgYDVQQLLEwdSYWxlaWdoMR"/>
  <encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSib3DQEJARYbYm9zc0BicnFQ"
    Ekey="EwJVUzELMAkGA1UECBMCTk"/>
</encrypt:class>

<empl_name>
  John Q. Smith
</empl_name>
<ser_nbr">
  E135246
</ser_nbr>
<date_of_hire>
  01/01/1980
</date_of_hire>
<curr_salary>
  <encrypt:data class="1">
    Ym0uY29tMQ
  </encrypt:data>
</curr_salary>
<medical_condition>
  <encrypt:data class="2">
    MxODAKBgNVB
  </encrypt:data>
</medical_condition>

```

Fig. 4C

Key Object - internal

500

distinguished name 501	X.509 certificate 502a	encrypted symmetric key 503
------------------------------	------------------------------	--------------------------------------

version number 501	serial number 502a	signature info 503	issuer 504	validity period 505	subject 506	public key info 507	certificate signature 508
--------------------------	--------------------------	--------------------------	---------------	---------------------------	----------------	---------------------------	---------------------------------

algorithm 509	subject public key 510
------------------	---------------------------------

Key Object - transmitted

510

distinguished name 501	X.509 certificate key identifier 502b	encrypted symmetric key 503
------------------------------	--	--------------------------------------

Fig. 5A

00422430-102499

preprocessingKeyClass Object 520

encryption strength 521	key class object 522	plaintext symmetric key 523
-------------------------------	----------------------------	--------------------------------------

Fig. 5B

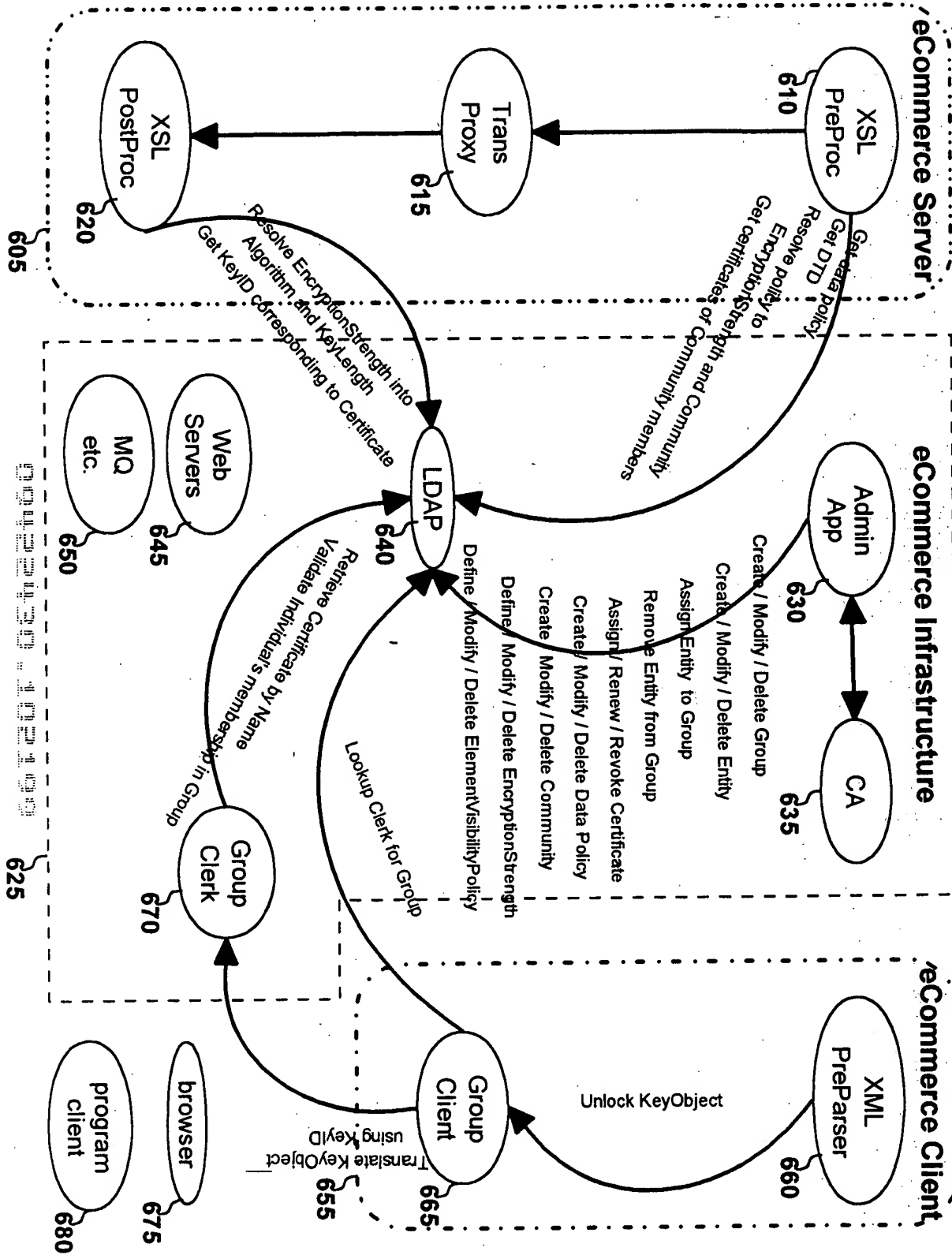
keyClass Object 530

class identifier 531	encryption algorithm identifier 532	key length 533	optional hints for algorithm 534	key object 1 535	key object 2 536	...	key object N 539
----------------------------	--	----------------------	--	------------------------	------------------------	-----	------------------------

Fig. 5C

0942430-102199

Fig. 6



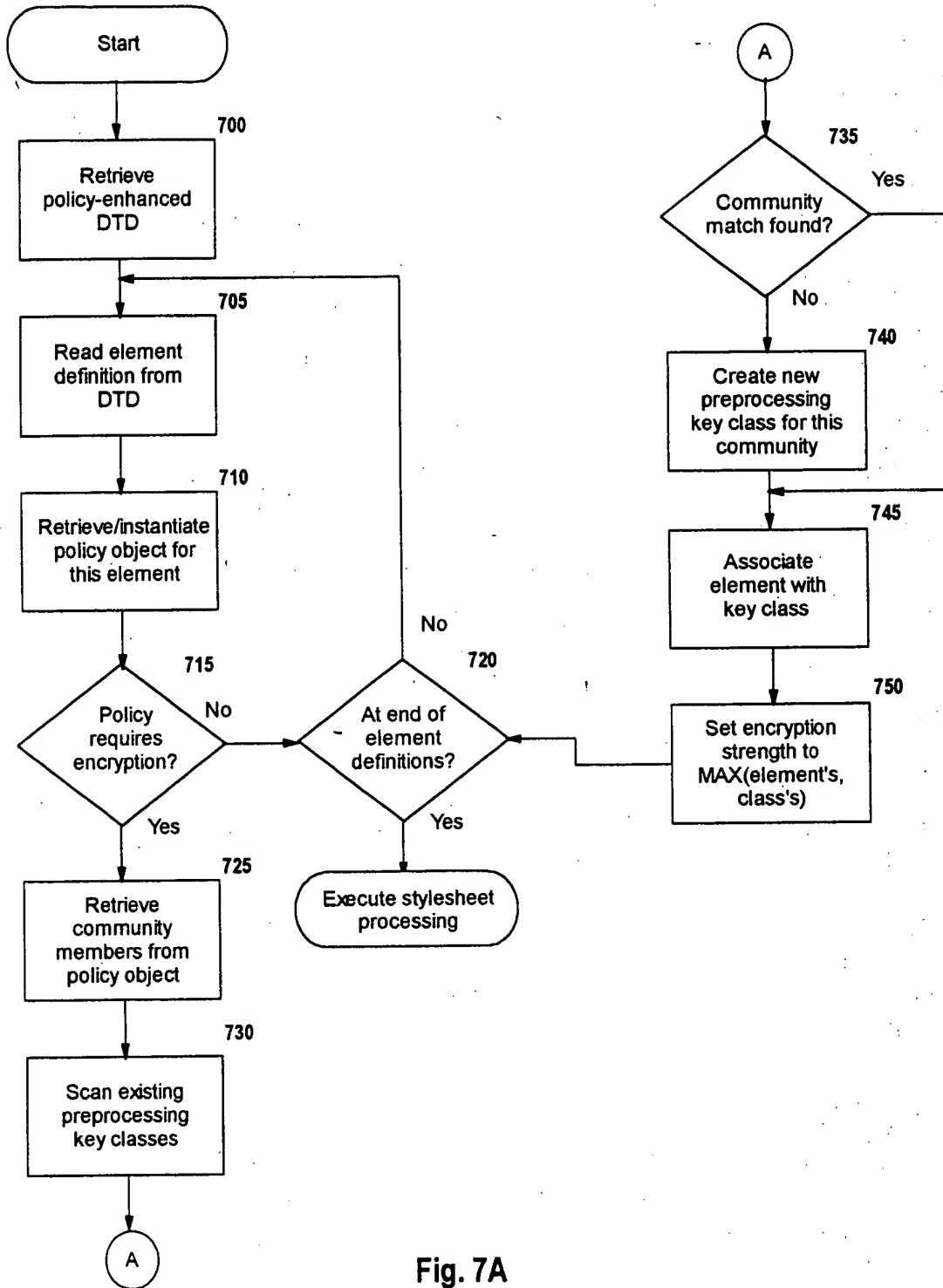


Fig. 7A

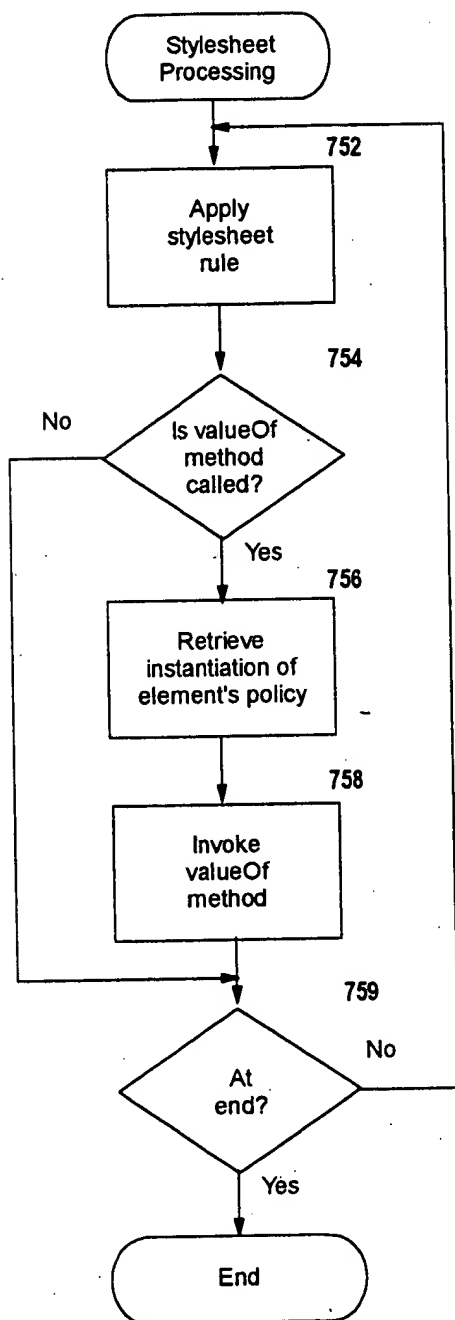


Fig. 7B

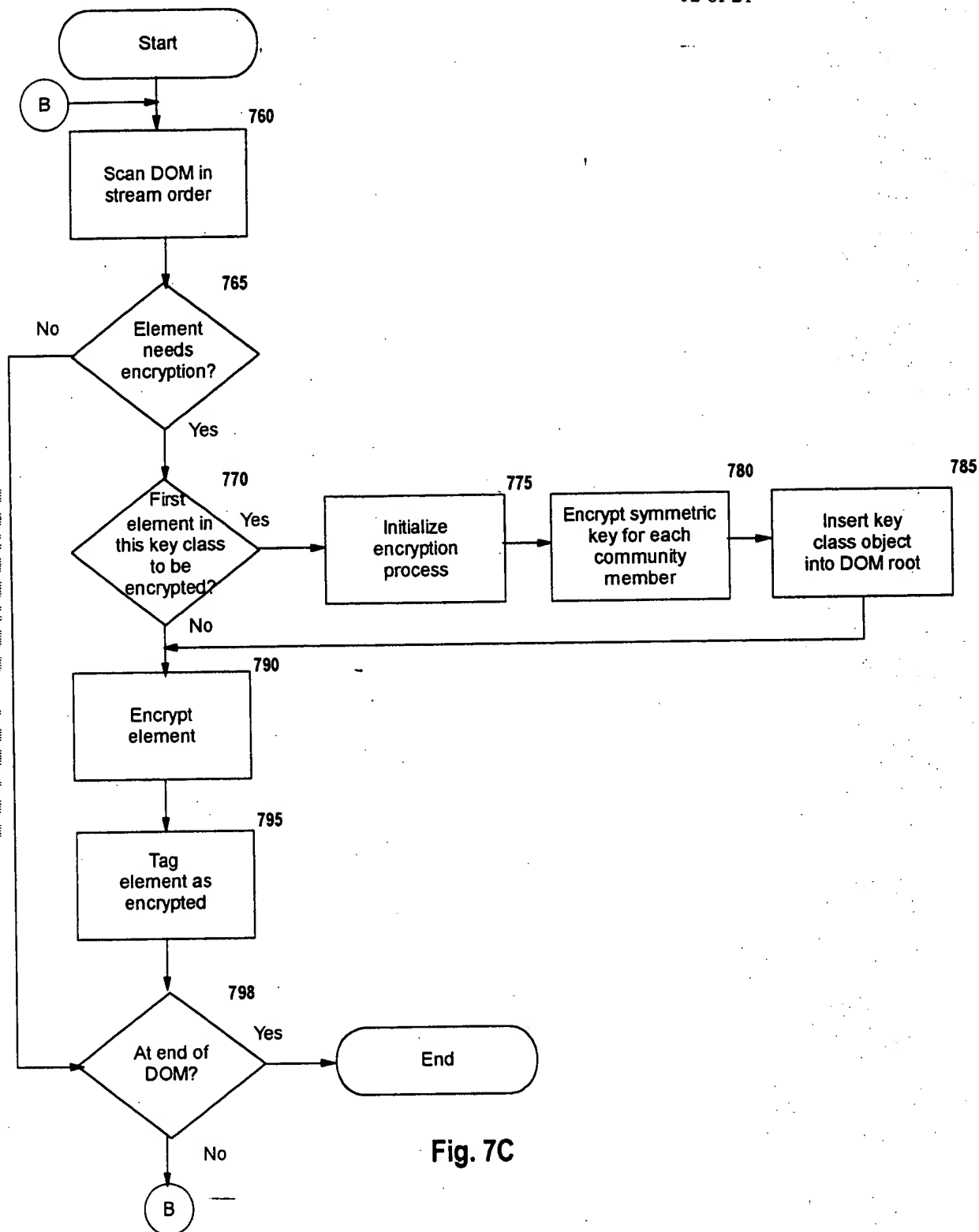


Fig. 7C

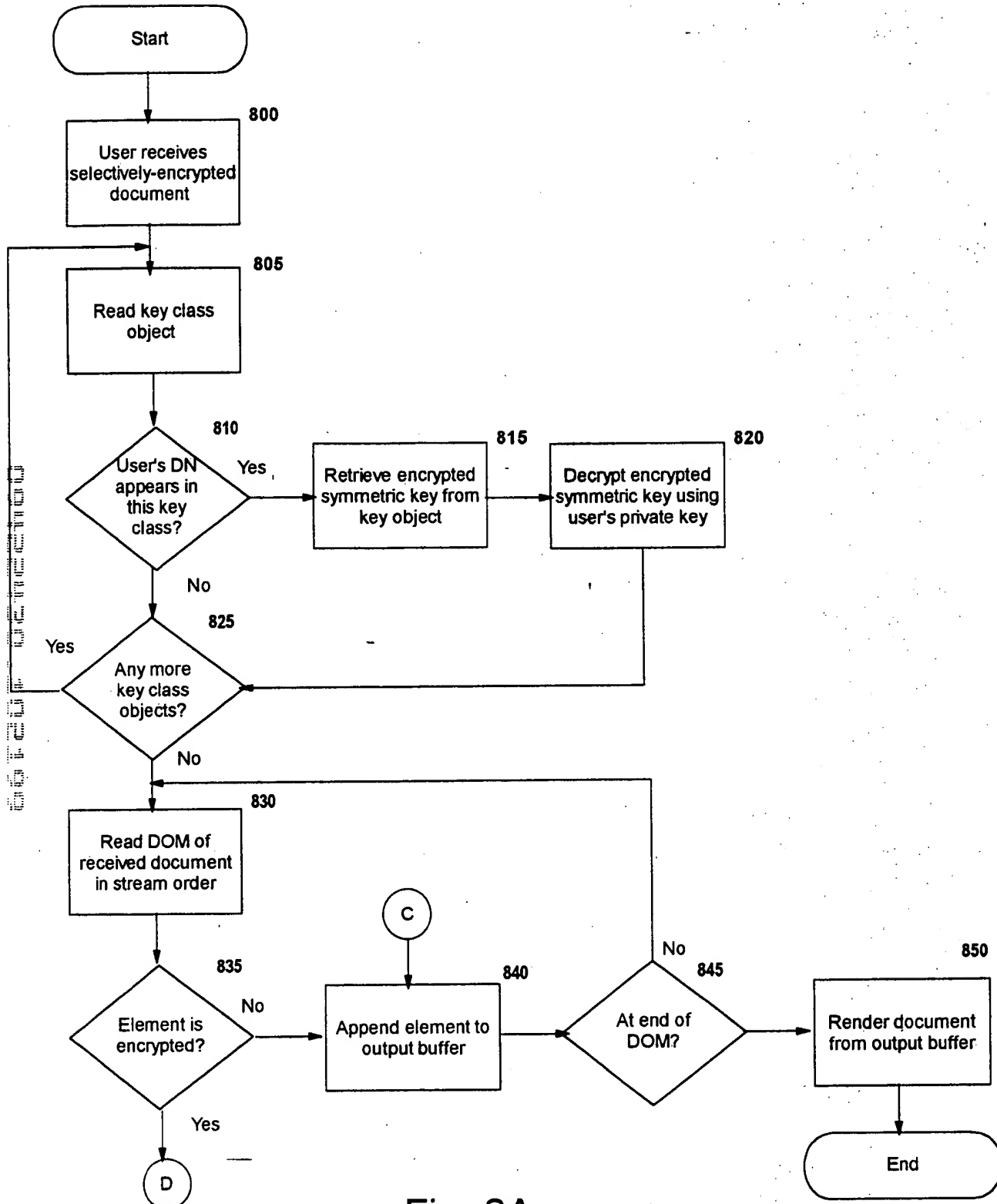


Fig. 8A

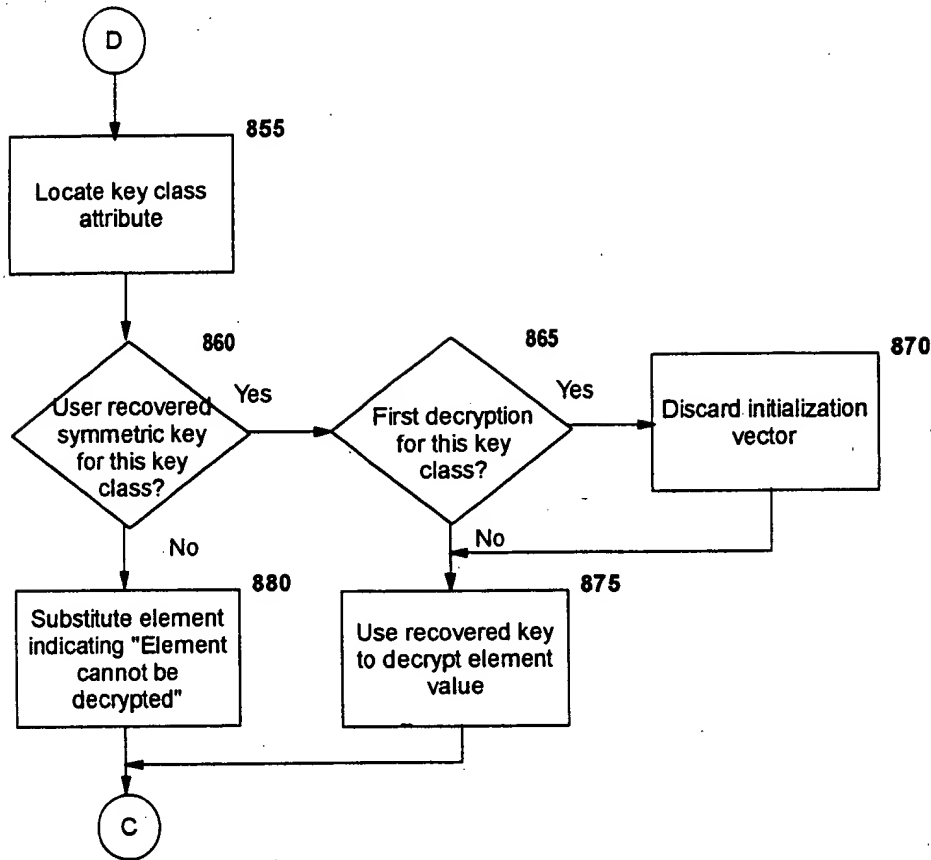


Fig. 8B

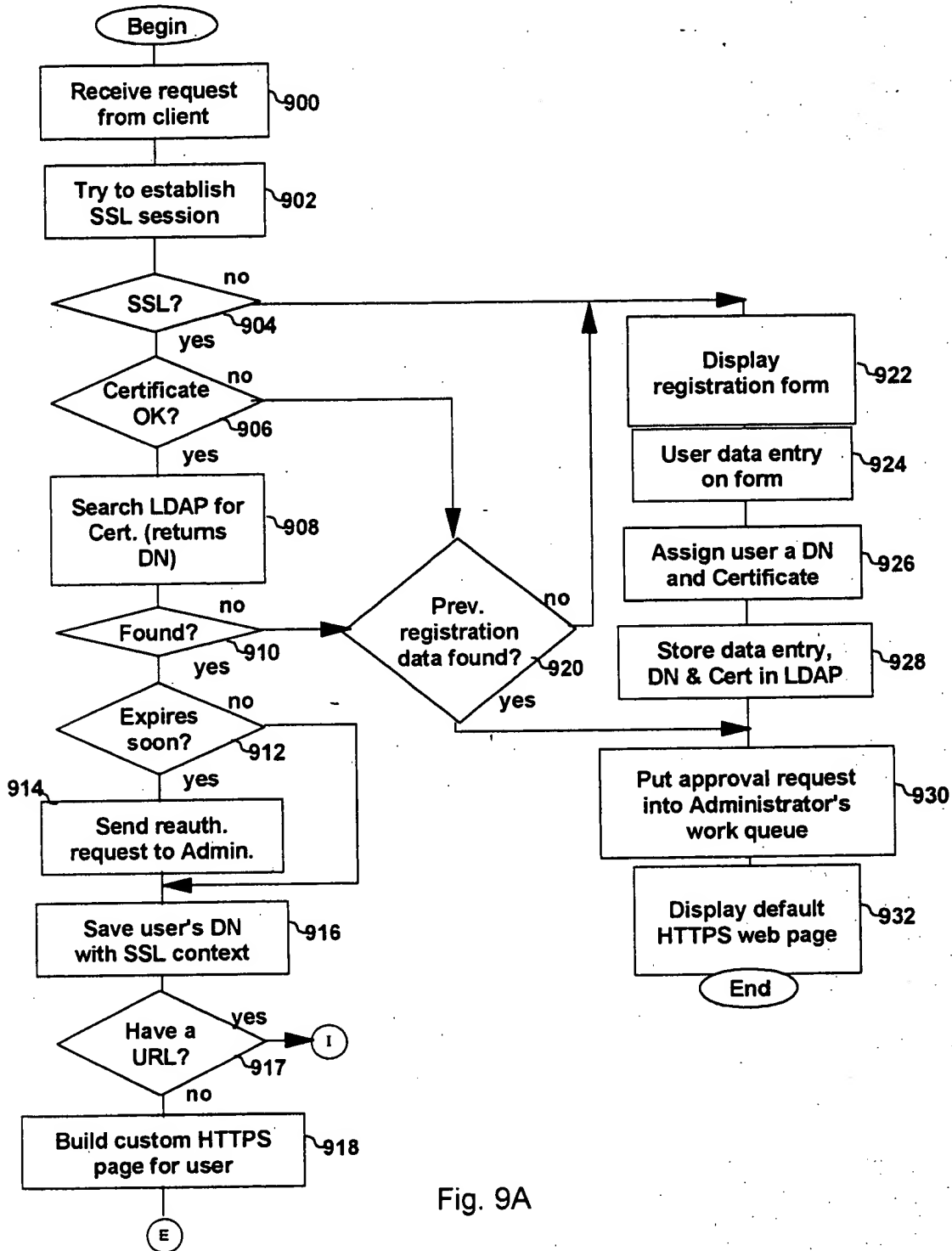


Fig. 9A



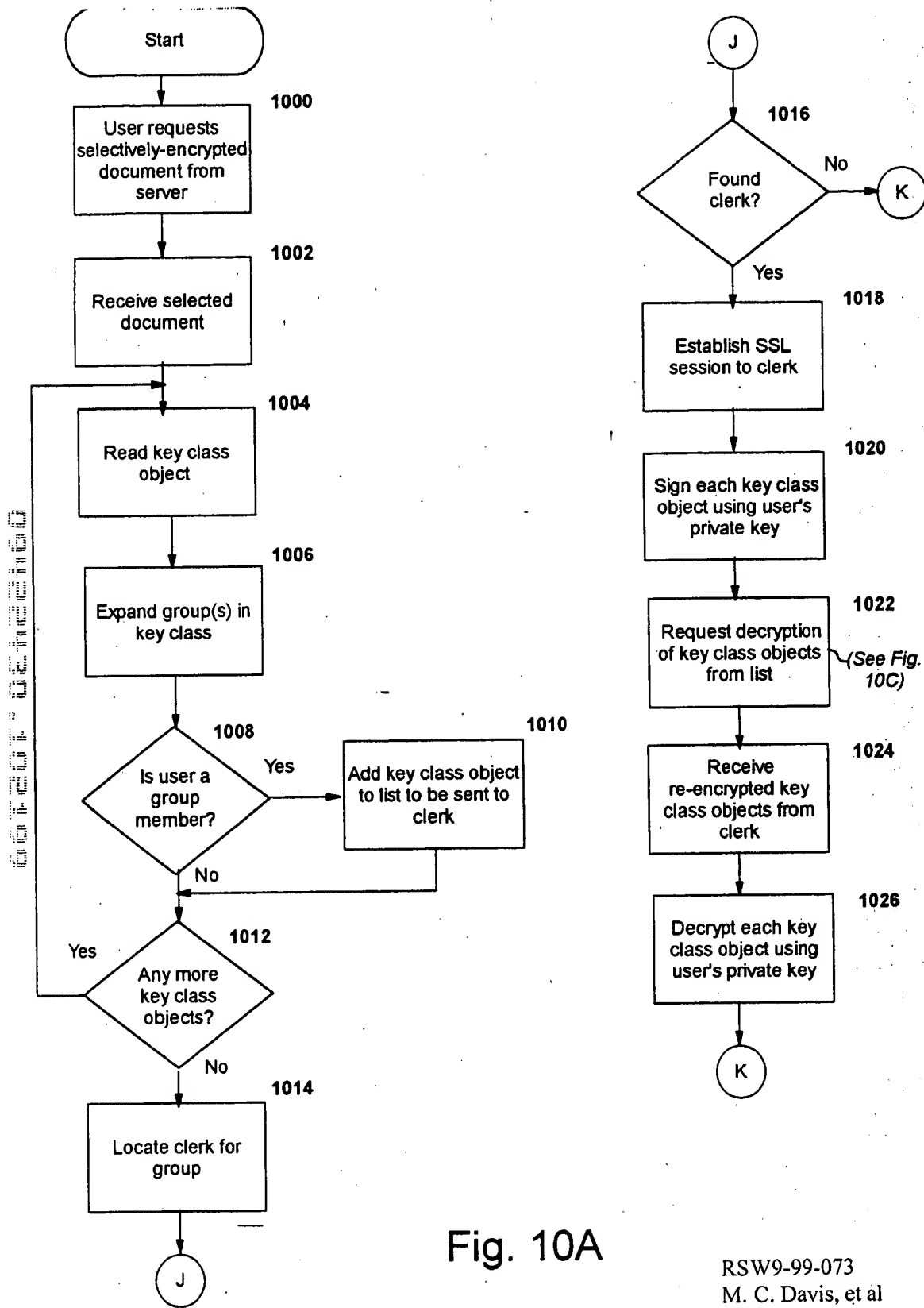


Fig. 10A

607207 0012100

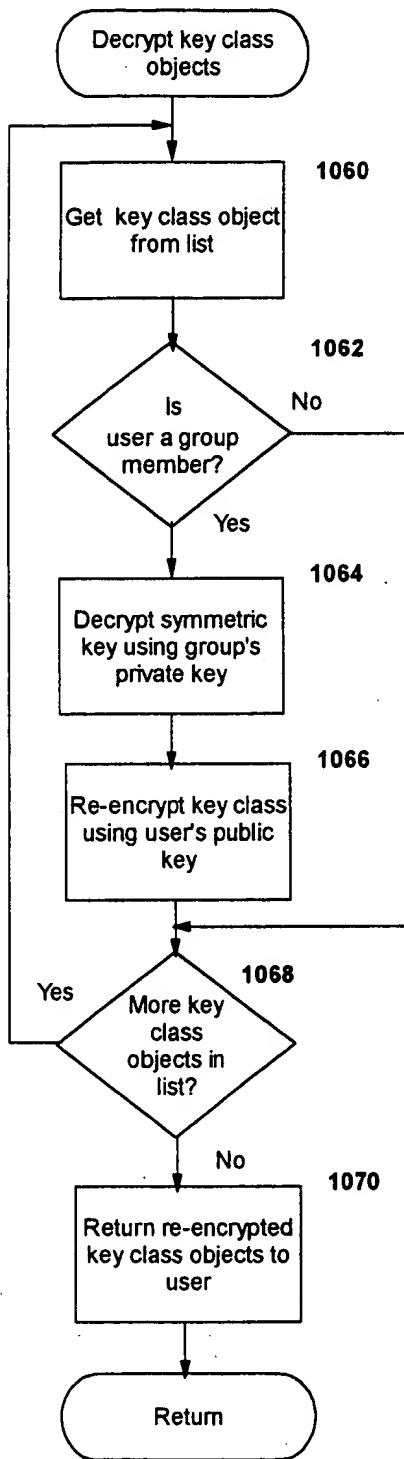


Fig. 10C

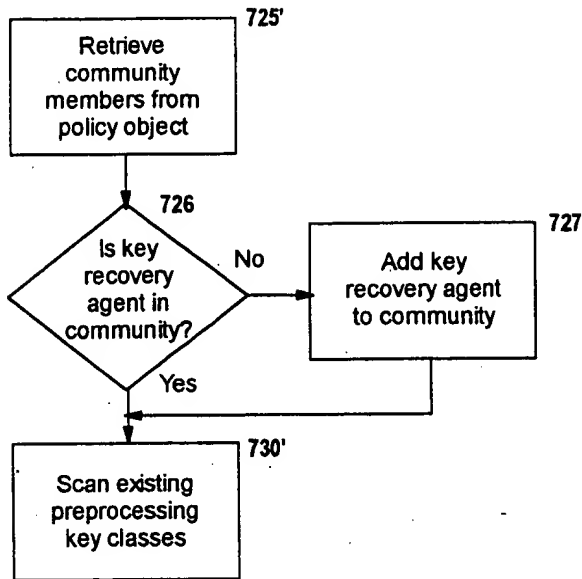


Fig. 11A

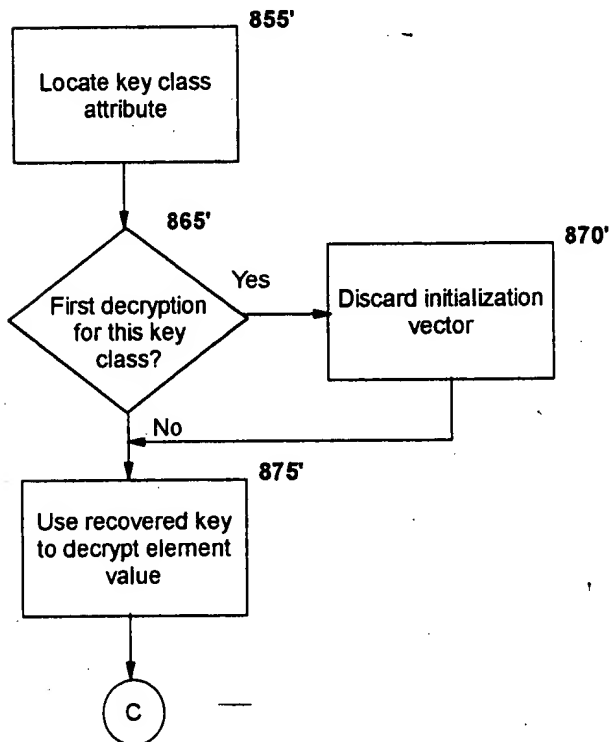


Fig. 11B

Fig. 12

